CRYPTOME

Donate for the Cryptome archive of files from June 1996 to the present

---

21 September 2014. Apple and Spy Disbelief:

http://cryptome.org/2014/09/apple-spy-disbelief.htm

Google and Apple Subverting Device Encryption?:

http://cryptome.org/2014/09/google-apple-crypto.pdf

20 September 2014

Apple Wiretap Disbelief

To: cryptography[at]metzdowd.com
Date: Fri, 19 Sep 2014 21:16:01 -0700
From: John Gilmore <gnu[at]toad.com>
Subject: Re: [Cryptography] new wiretap resistance in iOS 8?

> > Quoting from the new iOS 8 privacy policy announced tonight Wed Sep 17.
> > > Apple has no way to decrypt iMessage and FaceTime data when it is in
> > > transit between devices. So unlike other companies' messaging
> > > services, Apple doesn't scan your communications, and we wouldn't be
> > > able to comply with a wiretap order even if we wanted to.
> > https://www.apple.com/privacy/privacy-built-in/

And why do we believe them?

* Because we can read the source code and the protocol descriptions ourselves, and determine just how secure they are?

* Because they're a big company and big companies never lie?

* Because they've implemented it in proprietary binary software, and proprietary crypto is always stronger than the company claims it to be?

* Because they can't covertly send your device updated software that would change all these promises, for a targeted individual, or on a mass basis?

* Because you will never agree to upgrade the software on your device, ever, no matter how often they send you updates?

* Because this first release of their encryption software has no security bugs, so you will never need to upgrade it to retain your privacy?

* Because if a future update INSERTS privacy or security bugs, we will surely be able to distinguish these updates from future updates that FIX privacy or security bugs?

* Because if they change their mind and decide to lessen our privacy for their convenience, or by secret government edict, they will be sure to let us know?

* Because they have worked hard for years to prevent you from upgrading the software that runs on their devices so that YOU can choose it and control it instead of them?

* Because the US export control bureacracy would never try to stop Apple from selling secure mass market proprietary encryption products across the border?

* Because the countries that wouldn't let Blackberry sell phones that communicate securely with your own corporate servers, will of course let Apple sell whatever high security non-tappable devices it wants to?

* Because we're apple fanboys and the company can do no wrong?

* Because they want to help the terrorists win?

* Because NSA made them mad once, therefore they are on the side of the public against NSA?

* Because it's always better to wiretap people after you convince them that they are perfectly secure, so they'll spill all their best secrets?

There must be some other reason, I'm just having trouble thinking of it.

John
